PATENT ABSTRACTS OF JAPAN

(11)Publication number : **11-262059**
(43)Date of publication of application : **24.09.1999**

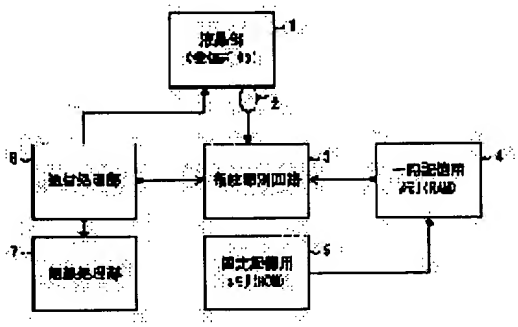
(51)Int.CI. **H04Q 7/38**

(21)Application number : **10-078592**
(22)Date of filing : **12.03.1998**

(71)Applicant : **NEC MOBILE COMMUN LTD**
(72)Inventor : **MIZUKURE HISAMI**

(54) PORTABLE TERMINAL FOR MOBILE COMMUNICATION AND PERSONAL IDENTIFICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent a portable terminal from unauthorized use by a 3rd party.
SOLUTION: Fingerprint data of a user are stored in a ROM inside of the portable terminal in advance as personal ID data. At the application of power to the portable terminal, the personal ID data stored in the ROM 5 are expanded in a RAM 4 that is accessed at high speed. After the depression of a dial button 1 with a fingerprint identification sensor 2 mounted thereon in a portable terminal liquid crystal display section 1, a telephone number is entered and the dial button 1 of the liquid crystal display section is depressed again to conduct dialing processing. In this dialing procedure, when at first the dial button 1 is depressed, the fingerprint identification sensor 2 reads the fingerprint of the user, converts the pattern into a dot pattern as data. The acquired finger print data are collated with the personal ID data which have been stored as fingerprint data, when the portable terminal is purchased. When they do not match, dialing is made disable. Only if they match, is the entry of the telephone number is permitted and the dial processing conducted.



LEGAL STATUS

[Date of request for examination]	12.03.1998
[Date of sending the examiner's decision of rejection]	30.11.1999
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[The technical field to which invention belongs] this invention relates to the method of preventing disclosure of the data memorized in the unauthorized use or the personal digital assistant, by performing a user's identification about terminal equipments (henceforth a personal digital assistant), such as a cellular phone used for mobile communications.
[0002]
[Description of the Prior Art] Although there is a method prevent from using unless it sets up a personal identification number or a password and a personal identification number in agreement is inputted, as any men other than the owner cannot use a personal digital assistant without notice conventionally, when the 3rd person gets to know a personal identification number or a password, this 3rd person will be possible [using the personal digital assistant improperly].
[0003] The method of preventing the unauthorized use of devices, such as a cellular phone, is indicated by judging whether you are a regular user, and making JP,9-84128,A interrupt a telephone call by equipping a personal digital assistant with the function to recognize an owner's voice, parameterizing the voice under telephone call, and comparing with the parameter memorized beforehand, in order to prevent the unauthorized use of such a personal digital assistant, if it is not a regular user.
[0004] By the method indicated by this open official report, if the power supply of a personal digital assistant is turned on, it will become personal identification number input mode, and if the right personal identification number is inputted, a dial lock is canceled and it will be in the waiting receptacle for reception, and a dial call origination state. If the partner point telephone number is inputted from a keyboard in this state and a circuit is connected with the partner point, it will be in a talk state and a telephone call will be started. The voice under this telephone call is changed into a voice sign parameter, and is compared with the voice sign parameter beforehand registered into memory by the personal digital assistant owner. Although a line connection state will be continued as it is as a result of comparison if in agreement, when inharmonious, a circuit is cut and it will be in a dial lock state.
[0005]
[Problem(s) to be Solved by the Invention] Since according to the unauthorized use prevention means indicated by the aforementioned open official report a user's voice sign parameter differs from the voice sign parameter registered beforehand even if a personal identification number etc. will be known, a line connection will be carried out unjustly and it will be in a talk state Although it becomes impossible to cut a circuit and to continue the telephone call beyond it and an unauthorized use can be prevented By this method, there is a fault that it cannot judge whether it is an unauthorized use, and there is a problem that phonecall charges must be paid, in spite of the unauthorized use by the third person until it carries out a line connection and a telephone call is performed.
[0006] By performing identification by the simple operation which solved the above-mentioned technical problem, this invention prevents the unjust use by the improvement in security and the third person to the

data memorized by the cellular phone, and aims at suppressing the damage at the time of loss etc. to the minimum.
[0007]
[Means for Solving the Problem] this invention carries the circuit and sensor for performing identification based on physical information to a personal digital assistant, acquires the aforementioned identification information in advance of the use after switching on the power supply of a personal digital assistant, collates it with the individual ID data memorized beforehand, and when inharmonious, it makes use of a personal digital assistant improper.
[0008] In performing identification by the fingerprint, using a fingerprint as physical information, it considers as the composition which has a fingerprint discernment sensor in the dispatch button of a personal digital assistant, or a part of liquid crystal section, and when a user touches the sensor section with a finger at the time of dispatch etc., a user's fingerprint is acquired, and it collates with the fingerprint data memorized beforehand.
[0009] Moreover, like the aforementioned official report publication, when performing identification with voice, a user's speech information is acquired in advance of the use, and it collates with the voice data memorized beforehand, and in being inharmonious, it makes a telephone number input improper.
[0010]
[Embodiments of the Invention] Drawing 1 is the block diagram showing the gestalt of operation of this invention, and shows the example applied to the personal digital assistant of mobile communications. Beforehand, physical individual ID data, such as a user's fingerprint, are stored in the personal digital assistant of this invention in the memory 5 (henceforth ROM) for fixed storage, and this individual ID data is developed in the memory 4 (henceforth RAM) for temporary storage at the power up at it (at the time of personal digital assistant purchase etc.).
[0011] Some liquid crystal screens are equipped with the dispatch button 1 of a touch-panel method, and the fingerprint discernment sensor 2 is carried in a personal digital assistant. The interior of a personal digital assistant has the communications processing section 6 and the radio processing section 7 like the conventional terminal, and has the fingerprint discrimination decision circuit 3 which processes this invention further.
[0012] Next, operation of this invention is explained with reference to drawing 1 and drawing 2 . ROM5 inside a personal digital assistant is made to memorize a user's fingerprint data as individual ID data beforehand. An injection of the power supply of a personal digital assistant develops the individual ID data memorized by ROM5 on RAM4 in which rapid access is possible. The telephone number is inputted for the dispatch button 1 carrying the fingerprint discernment sensor 2 in the personal digital assistant liquid crystal section 1 after a depression, and dispatch processing is again performed by carrying out the depression of the dispatch button 1 of the liquid crystal section.
[0013] In this dispatch procedure, when the dispatch button 1 is pushed first, a user's fingerprint is read by the fingerprint discernment sensor 2, and the configuration is changed into a dot pattern and is data-ized. In addition, when the depression position has shifted, it asks for the center position of a fingerprint, and amendment is applied.
[0014] The acquired fingerprint data are collated with the individual ID data made to memorize as fingerprint data when a personal digital assistant is purchased, and when inharmonious, they presuppose that dispatch is impossible. Only when in agreement, the input of the telephone number is permitted, and dispatch processing is performed.
[0015] If depression operation of the dispatch button before a telephone number input is performed, since fingerprint detection and discernment processing will be made automatically according to this invention, there is also no object for ** which performs operation that it is special for fingerprint collating, and identification can be performed by simple operation.
[0016] In addition, in a terminal unit given in drawing 1 , although ROM5 inside a personal digital assistant is made to memorize a user's fingerprint data as individual ID data beforehand The PC card type IC card is made to memorize these individual ID data, and it is inserted in a personal digital assistant, and

when the dispatch button in the liquid crystal portion of a personal digital assistant is pushed, it can also consider as the composition which collates a user's acquired fingerprint data and the individual ID data in an IC card.

[0017] It becomes possible such composition, then to share one set of a personal digital assistant by two or more men who hold each people's PC card type IC card, respectively. Furthermore, if this IC card is communalized with the personal computer and gate system which perform fingerprint discernment, convenience will improve further.

[0018] In the gestalt of the above-mentioned operation, although discernment by the fingerprint is performed as the identification method, it is also possible to carry out by discernment with voice. Drawing 3 is a flowchart in which operation in the case of performing discernment with voice is shown. Namely, encode individual voice beforehand, the internal memory (ROM) or IC card of a personal digital assistant is made to memorize by making it into individual ID data like the case of the above-mentioned fingerprint discernment, and the ID data is loaded to RAM at the time of personal digital assistant use. And a user's opening words (password etc.) are data-ized at the time of a dispatch button depression, it collates with the personal data in RAM, if in agreement, a telephone number input will be permitted, and if inharmonious, suppose that dispatch is impossible.

[0019]

[Effect of the Invention] When the 3rd person other than those by whom physical individual ID data, such as a fingerprint and voice, are beforehand registered even when a personal digital assistant is lost tries to send according to this invention, since it can collate and dispatch is impossible, disclosure of the data memorized in the unauthorized use by the 3rd person or the personal digital assistant etc. can be prevented, and the damage at the time of personal digital assistant loss can be pressed down to the minimum. Moreover, improvement in security can be aimed at.

[0020]

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（A）**　(11)特許出願公開番号

特開平11－262059

(43)公開日　平成11年(1999)９月24日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｓ

審査請求　有　　請求項の数７　ＦＤ　（全　４　頁）

(21)出願番号　特願平10－78592

(22)出願日　平成10年(1998)３月12日

(71)出願人　390000974
日本電気移動通信株式会社
横浜市港北区新横浜三丁目16番８号　（ＮＥＣ移動通信ビル）

(72)発明者　水呉　久美
神奈川県横浜市港北区新横浜３丁目16番８号　日本電気移動通信株式会社内

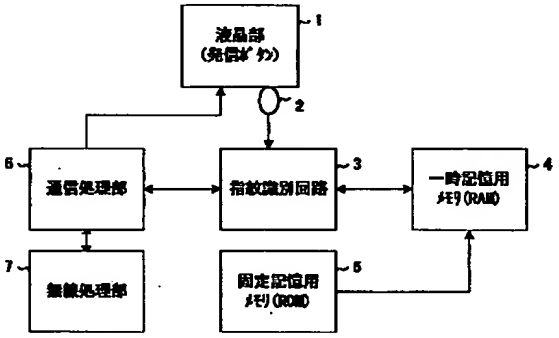
(74)代理人　弁理士　鈴木　康夫　（外１名）

(54)【発明の名称】　移動通信用携帯端末及び個人識別方法

(57)【要約】

【課題】　携帯端末を第３者により不正使用されることを防止する。

【解決手段】　携帯端末内部のＲＯＭ５には予め使用者の指紋データを個人ＩＤデータとして記憶させておく。携帯端末の電源が投入されると、ＲＯＭ５に記憶されている個人ＩＤデータを高速アクセスが可能なＲＡＭ４上に展開する。携帯端末液晶部１にある指紋識別センサー２を搭載した発信ボタン１を押下後、電話番号を入力し、再度、液晶部の発信ボタン１を押下することにより発信処理を行う。この発信手順において、最初に発信ボタン１を押下した際に指紋識別センサー２で使用者の指紋を読みとり、その形状をドットパターンに変換し、データ化する。取得した指紋データは、携帯端末を購入した時に指紋データとして記憶させた個人ＩＤデータと照合され、不一致だった場合には発信不可とする。一致した場合のみ電話番号の入力を許可し、発信処理を行う。



1

【特許請求の範囲】

【請求項１】　移動通信に用いられる携帯端末において、

前記携帯端末は、身体的情報に基づく個人識別情報を記憶する記憶手段と、前記携帯端末からの発信操作に連動して使用者の前記身体的情報を取得する識別情報取得手段と、前記記憶手段に記憶されている個人識別情報と前記識別情報取得手段によって取得された前記身体的情報とを比較する比較手段と、前記比較手段による比較結果に基づいて前記発信の可又は不可を決定する手段を備えていることを特徴とする移動通信用携帯端末。

【請求項２】　前記身体的情報に基づく個人識別情報は、指紋データであることを特徴とする請求項１記載の移動通信用携帯端末。

【請求項３】　前記識別情報取得手段は、前記携帯端末の発信操作を行う発信釦に配置された指紋識別センサーと、該指紋識別センサーによって読み取られた指紋を指紋データに変換する手段とからなることを特徴とする請求項２記載の移動通信用携帯端末。

【請求項４】　前記身体的情報に基づく個人識別情報は、音声データであることを特徴とする請求項１記載の移動通信用携帯端末。

【請求項５】　移動通信に用いられる携帯端末において、身体的情報に基づく個人識別情報が記録されているＩＣカードを携帯端末本体に挿入し、前記ＩＣカードに記憶されている前記個人識別情報と発信開始時に取得した使用者の身体的情報に基づく個人識別情報とを照合することを特徴とする移動通信用携帯端末における個人識別方法。

【請求項６】　前記身体的情報に基づく個人識別情報は、指紋データであることを特徴とする請求項５記載の移動通信用携帯端末における個人識別方法。

【請求項７】　前記身体的情報に基づく個人識別情報は、音声データであることを特徴とする請求項５記載の移動通信用携帯端末における個人識別方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、移動体通信に用いられる携帯電話等の端末機器（以下、携帯端末という）に関し、使用者の個人識別を行うことにより、不正使用や携帯端末内に記憶されているデータの漏洩を防止する方法に関する。

【０００２】

【従来の技術】従来、携帯端末をその所有者以外の人が無断で使用できないように、暗証番号あるいはパスワードを設定し、一致する暗証番号が入力されない限り使用できないようにする方法があるが、暗証番号あるいはパスワードを第３者に知られてしまった場合には、この第３者がその携帯端末を不正使用することが可能となってしまう。

2

【０００３】このような携帯端末の不正使用を防止するために、特開平９－８４１２８号公報には、携帯端末に所有者の音声を認識する機能を備え、通話中の音声をパラメータ化し、予め記憶されたパラメータと比較することにより、正規の使用者か否かを判断し、正規の使用者でなければ通話を中断させることにより、携帯電話等の機器の不正使用を防ぐ方法が開示されている。

【０００４】この公開公報に記載されている方法では、携帯端末の電源がＯＮされると、暗証番号入力モードとなり、正しい暗証番号が入力されるとダイヤルロックが解除され、受信待ち受け及びダイヤル発呼状態となる。この状態でキーボードから相手先電話番号が入力され、相手先と回線が接続されると通話状態になり、通話が開始される。この通話中の音声は音声符号パラメータに変換されて、携帯端末所有者によって予めメモリに登録された音声符号パラメータと比較される。比較の結果、一致すればそのまま回線接続状態が継続されるが、不一致の場合には回線が切断され、ダイヤルロック状態となる。

【０００５】

【発明が解決しようとする課題】前記公開公報に記載されている不正使用防止手段によれば、暗証番号等が知られて不正に回線接続され、通話状態となっても、使用者の音声符号パラメータが予め登録されている音声符号パラメータとは異なるので、回線は切断され、それ以上の通話を継続することはできなくなり、不正使用を防止することができるが、この方法では、回線接続して通話が行われるまでは、不正使用であるか否かを判断することができないという欠点があり、第三者による不正使用にも拘わらず通話料金を負担しなければならないという問題がある。

【０００６】本発明は、上記の課題を解決した簡易な操作で個人識別を行うことにより、携帯電話に記憶されているデータに対するセキュリティの向上および第三者による不当な使用を防止し、紛失時等の被害を最小限に抑えることを目的とするものである。

【０００７】

【課題を解決するための手段】本発明は、携帯端末に身体的情報に基づく個人識別を行うための回路やセンサーを搭載し、携帯端末の電源を投入後、その使用に先だって前記個人識別情報を取得し、あらかじめ記憶されている個人ＩＤデータと照合を行い、不一致の場合には、携帯端末の使用を不可とするものである。

【０００８】身体的情報として指紋を用い、指紋による個人識別を行う場合には、携帯端末の発信ボタンあるいは液晶部の一部に指紋識別センサーを有する構成とし、発信時などに使用者がそのセンサー部を指で触れることにより使用者の指紋を取得し、予め記憶されている指紋データと照合を行う。

【０００９】また、前記公報記載のように、音声による

個人識別を行う場合には、その使用に先だって使用者の音声情報を取得し、あらかじめ記憶されている音声データと照合を行い、不一致の場合には、電話番号入力を不可とするものである。

【００１０】

【発明の実施の形態】図１は、本発明の実施の形態を示すブロック図であり、移動体通信の携帯端末に適用した例を示している。本発明の携帯端末には、あらかじめ（携帯端末購入時などに）使用者の指紋などの身体的な個人ＩＤデータを固定記憶用メモリ５（以下、ＲＯＭという）に記憶させておき、電源投入時には、この個人ＩＤデータを一時記憶用メモリ４（以下、ＲＡＭという）に展開しておく。

【００１１】携帯端末には、液晶画面の一部分にタッチパネル方式の発信ボタン１が備えられ、指紋識別センサー２が搭載される。携帯端末内部は、従来の端末同様に通信処理部６と無線処理部７を有し、さらに本発明の処理を行う指紋識別回路３を有している。

【００１２】次に、本発明の動作について、図１および図２を参照して説明する。携帯端末内部のＲＯＭ５にはあらかじめ使用者の指紋データを個人ＩＤデータとして記憶させておく。携帯端末の電源が投入されると、ＲＯＭ５に記憶されている個人ＩＤデータを高速アクセスが可能なＲＡＭ４上に展開する。携帯端末液晶部１にある指紋識別センサー２を搭載した発信ボタン１を押下後、電話番号を入力し、再度、液晶部の発信ボタン１を押下することにより発信処理を行う。

【００１３】この発信手順において、最初に発信ボタン１を押下した際に指紋識別センサー２で使用者の指紋を読みとり、その形状をドットパターンに変換し、データ化する。なお、押下位置がずれている場合には指紋の中心位置を求め、補正をかけるようにする。

【００１４】取得した指紋データは、携帯端末を購入した時に指紋データとして記憶させた個人ＩＤデータと照合され、不一致だった場合には発信不可とする。一致した場合のみ電話番号の入力を許可し、発信処理を行う。

【００１５】本発明によれば、電話番号入力に先立つ発信ボタンの押下操作を行うと、自動的に指紋検出及び識別処理がなされるので、指紋照合のために特別の操作を行う必用もなく、簡易な操作で個人識別を行うことができる。

【００１６】なお、図１記載の端末装置においては、携帯端末内部のＲＯＭ５にはあらかじめ使用者の指紋データを個人ＩＤデータとして記憶させているが、これらの個人ＩＤデータをＰＣカードタイプのＩＣカードに記憶させておき、それを携帯端末に挿入し、携帯端末の液晶部分にある発信ボタンが押下された際に、取得した使用者の指紋データとＩＣカード内の個人ＩＤデータとを照合する構成とすることもできる。

【００１７】このような構成とすれば、それぞれ各個人のＰＣカードタイプのＩＣカードを保持する複数の人によって一台の携帯端末を共用することが可能となる。さらに、このＩＣカードを、指紋識別を行うパソコンやゲートシステムと共通化すれば利便性は一層向上する。

【００１８】上記の実施の形態においては、個人識別方法として指紋による識別を行っているが、音声による識別で行うことも可能である。図３は、音声による識別を行う場合の動作を示すフローチャートである。すなわち、上記指紋識別の場合と同様に、あらかじめ個人の音声を符号化し、それを個人ＩＤデータとして携帯端末の内部メモリ（ＲＯＭ）もしくはＩＣカードに記憶させておき、携帯端末使用時にそのＩＤデータをＲＡＭにロードする。そして、発信ボタン押下時に使用者の第一声（パスワードなど）をデータ化し、ＲＡＭ内の個人データと照合を行い、一致すれば電話番号入力を許可し、不一致であれば発信不可とする。

【００１９】

【発明の効果】本発明によれば、携帯端末を紛失した場合でも、あらかじめ指紋や音声などの身体的な個人ＩＤデータが登録されている人以外の第３者が発信しようとした場合、照合を行い、発信不可とすることが出来るため、第３者による不正使用や携帯端末内に記憶されているデータの漏洩などを防止することができ、携帯端末紛失時の被害を最小限に押さえることができる。また、セキュリティの向上を図ることができる。

【００２０】

【図面の簡単な説明】

【図１】本発明の実施の形態を示すブロック図である。

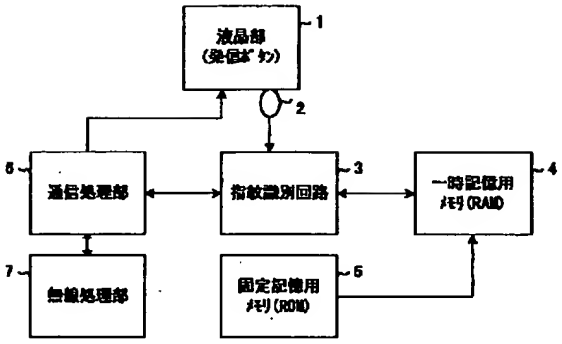
【図２】本発明の動作を説明するためのフローチャートである。

【図３】本発明の他の実施の形態の動作を説明するためのフローチャートである。

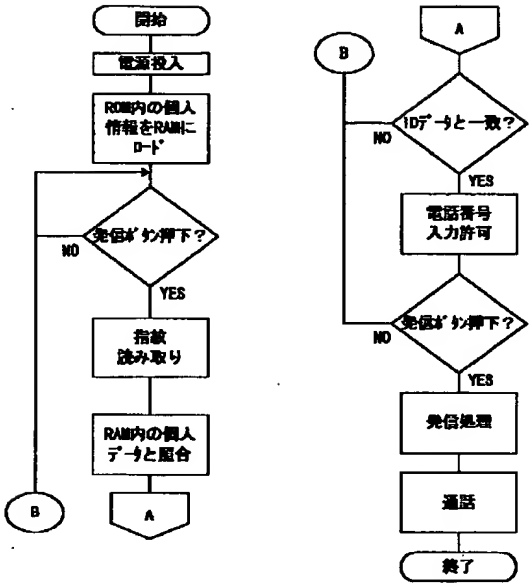
【符号の説明】

１　液晶部
２　指紋識別センサー
３　指紋識別回路
４　一時記憶用メモリ（ＲＡＭ）
５　固定記憶用メモリ（ＲＯＭ）
６　通信処理部
７　無線処理部

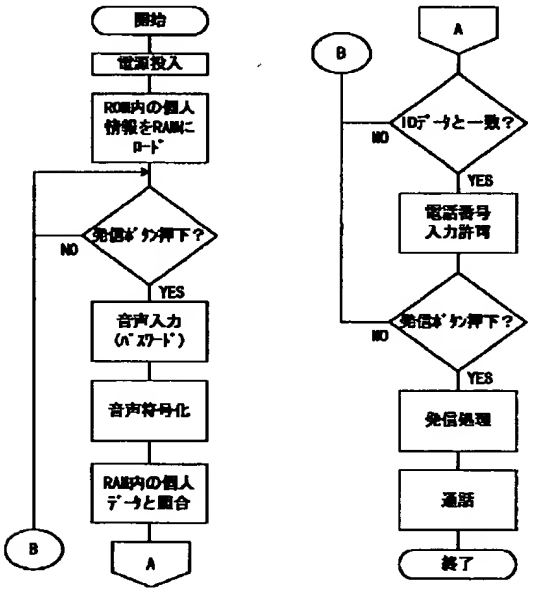
【図1】


液晶部
（発信ﾎﾞﾀﾝ）
1
2
通信処理部
指紋識別回路
3
一時記憶用
ﾒﾓﾘ(RAM)
4
6
7
無線処理部
固定記憶用
ﾒﾓﾘ(ROM)
5

【図2】


開始
電源投入
ROM内の個人
情報をRAMに
ﾛｰﾄﾞ
発信ﾎﾞﾀﾝ押下？
NO
YES
指紋
読み取り
RAM内の個人
ﾃﾞｰﾀと照合
B
A
IDﾃﾞｰﾀと一致？
電話番号
入力許可
通話
終了

【図3】


開始
電源投入
ROM内の個人
情報をRAMに
ﾛｰﾄﾞ
発信ﾎﾞﾀﾝ押下？
NO
YES
音声入力
（ﾊﾟｽﾜｰﾄﾞ）
音声符号化
RAM内の個人
ﾃﾞｰﾀと照合
B
A
IDﾃﾞｰﾀと一致？
電話番号
入力許可
発信処理
通話
終了